UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/364,835 | 07/30/1999 | BAIJU V. PATEL | INTL-0182-US | 9974 |

7590 07/28/2004

TIMOTHY N TROP
TROP PRUNER HU & MILES PC
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

| EXAMINER | |
|---|---|
| HA, LEYNNA A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | 15 |

DATE MAILED: 07/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/364,835 | PATEL ET AL. | |
| | Examiner | Art Unit | |
| | LEYNNA T. HA | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *07 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

**1.** Claims 1-27 has been re-examined and remains rejected under 35 U.S.C. 102(b). This is a FINAL rejection necessitated by new grounds of rejection.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

*A person shall be entitled to a patent unless –*

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**2. Claims 1-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Abadi, Et Al. (US 5,268,962).**

**As per claim 1:**

Abadi discloses a method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block; **(see col.3, lines 61-65 and col.4, lines 24-27; security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key**

**needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet.)**

generating security information to pass along with the data block, the security information identifying the security service; **and (see col.4, lines 28-68 and col.8, line 60 thru col.9, line 4; security information contained in the packet header includes key location, encrypted key value, key for encryption/decryption, and destination address, all of these information identifies the security service of the data packet)**

processing, in a computer peripheral device adapted to the communication with the communications channel, the data block according to the security information; **(see col.4, line 64 - col.5, line 33; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface.)**

**As per claim 2: see col.3, lines 61-65 and col.4, lines 24-27 (security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet);** discusses performing cryptographic processing of the data block.

**As per claim 3: see col.6, lines 7-63 and FIG.3;** discusses receiving the data block from a software routine and routing the processed data block back to the software routine after processing.

**As per claim 4: see col.7, line 63 – col.9, line 3;** discusses determining if the security service can be performed by the computer peripheral device and if not, processing the data block according to the security service in a software routine instead of the computer peripheral device.

**As per claim 5: see col.3, lines 55-65;** discussing the Internet Protocol Security.

**As per claim 6:**

Abadi discloses a method for use in a device including a computer peripheral device adapted to control communication with a transport medium, comprising **(FIG.3 and FIG.5b)**:

receiving data from a routine in the device; **(see col.4, lines 47-58 and col.5, lines 52-55)**

sending the data to the computer peripheral device to perform cryptographic processing. **(See col.5, lines 30-31 and col.6, lines 25-40 and 67-68; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface and cryptographic processing is the process of encryption or decryption.)**

**As per claim 7: see col.5, lines 1-33;** discusses sending the data to the computer peripheral device at least one more time to perform further cryptographic processing.

**As per claim 8:**

Abadi discloses a method for use in a device including a computer peripheral device adapted to control communication with a transport medium, comprising:

receiving data from the transport medium; **(see col.5, lines 52-55 and FIG.5a)**

determining from a portion of the data if cryptographic processing of the data is to be employed; and **(see col.5, line 52 thru col.6, line 23)**

performing, in the computer peripheral device, the cryptographic processing of data **(See col.4, lines 30-31 and col.6, lines 67-68; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface and cryptographic processing is the process of encryption or decryption.)**

**As per claim 9: see col.3, lines 61-65 and col.4, lines 24-27 (security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can**

**decrypt the packet);** discusses performing cryptographic processing is performed by a cryptographic engine in the computer peripheral device.

**As per claim 10: see col.7, line 63 – col.9, line 3;** discusses determining if the cryptographic processing can be performed by the computer peripheral device and performing the cryptographic processing in a software routine instead if the computer peripheral device is unable to perform the cryptographic processing.

**As per claim 11:**

Abadi discloses an article including a machine-readable storage medium containing instructions for execution in a system including a computer peripheral device adapted to control communication with a communications channel, the instructions when executed causing the system to **(FIG.3)**:

identify a security service to be performed on data to be transmitted over the communications channel; and **(see col.3, lines 61-65 and col.4, lines 24-27; security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet.)**

prepare security control information to pass along with the data to the computer peripheral device to perform processing according to the

identified security service. **(See col.4, lines 30-31 and col.6, lines 67-68; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface and cryptographic processing is the process of encryption or decryption.) (see col.3, lines 61-65 and col.4, lines 24-27; security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet.)**

**As per claim 12: see col.7, line 63 – col.9, line 3;** discussing the instructions causing the system to perform processing according to the identified security service instead of the computer peripheral device if the security service cannot be performed by the computer peripheral device.

**As per claim 13:**

Abadi discloses an article including a machine-readable storage medium containing instructions for execution in a system including a computer peripheral device adapted to control communication with a communications channel, the instructions when executed causing the system to **(see FIG.3)**:

receive a data block from the computer peripheral device; **(see col.5, lines 52-55)**

determine from information in the data block if a security service has not been performed on the data block by the computer peripheral device; and **(see col.3, lines 61-65 and col.4, lines 24-27; security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Abadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet.)**

process the data block if the security service has not been performed on the data block by the computer peripheral device. **(See col.4, lines 30-31 and col.6, lines 67-68; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface and cryptographic processing is the process of encryption or decryption.)**

**As per claim 14: see col.7, line 63 – col.9, line 3;** discussing the instructions causing the system to retrieve security information associated with the data block and sent the data block and security information to the computer peripheral device to perform the security service.

**As per claim 15: see col.6, lines 7-63;** discussing the instructions causing the system to perform the security service on the data block.

**As per claim 16:**

Abadi discusses a controller for controlling communications with a transport medium **(see FIG.3)**, the controller comprising:

a receiving circuit to receive data and associated security control information, the security control information identifying a security service to be performed on the data; and **(see col.3, lines 61-65, col.4, lines 24-27 and col.5, lines 46-55; security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet.)**

a cryptographic engine to cryptographically process the data based on the security control information, the cryptographic engine being in the computer peripheral device. **(See col.4, lines 30-31 and col.6, lines 67-68; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface and cryptographic processing is the process of encryption or decryption.)**

**As per claim 17:** Abadi discusses the storage device containing information identifying security services to be performed **(see col.3, lines 61-65 and col.4, lines 10-27)**, the received security control information selecting a portion of the security services information in the storage device **(see col.8 lines 3-44)**, wherein the cryptographic engine

processes the data according to the selected portion of the security services information. **(see col.5, lines 7-33 and col.9, lines 5-15)**

**As per claim 18:** **see col.8, lines 36-51;** discussing a device adapted to change the contents of the storage device to update the security services information. [it is inherent in the art that updating to make sure the system doesn't have outdated or unnecessary data and because updating inherently helps the security of a system further]

**As per claim 19:** **see col.8, lines 36-51;** discussing a device adapted the security services information based on a predetermined replacement policy.

**[it is inherent in the art that a replacement policy to makes sure the system doesn't have outdated or unnecessary data that would cause the system to slow down or takes longer period of time to process and because a replacement policy inherently further helps the security of a system]**

**As per claim 20:** **see col.8, lines 5-44;** discussing the security services information includes security association information.

**As per claim 21:**

Abadi discloses a device coupled to a communications channel, comprising:

an entity capable of generating data for transmission to the communications channel; and **(see col.3, lines 61-65 and FIG.3)**

a computer peripheral device adapted to control communications between the entity and the communications channel **(see FIG.6)**, the

controller including an engine to modify data according to the security protocol before transmitting the data to the communications channel **(See col.4, lines 30-31 and col.6, lines 67-68; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface and cryptographic processing is the process of encryption or decryption.)** and a receiving circuit to receive data from the communications channel and security data to identify if the received data is subject to cryptographic processing. **(see col.3, lines 61-65, col.5, lines 46-55 and col.6, lines 7-23; security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet. The values are compared and if valid, decryption of the packet proceeds on, but if invalid then it is discarded which inherently would not proceed further to the decryption step.)**

**As per claim 22: see col.5, lines 7-33;** discusses the engine is adapted to perform cryptographic processing.

**As per claim 23: see col.4, lines 10-13 and FIG.3;** discussing network controller.

**As per claim 24: see FIG.3 and FIG.6;** discussing the application process.

**As per claim 25:** Abadi discusses a routine adapted to generate predetermined security information used by the engine **(see col.7, line 63 – col.9, line 3)** to modify the data according to the security protocol **(see col.3, lines 55-65).**

**As per claim 26:** Abadi discusses a controller **(see col.4, lines 10-13)** includes a receiving circuit to receive data from the communications channel and security data to identify **(see col.5, lines 52-55)** if the received data is subject to cryptographic processing. **(see col.3, lines 61-65, col.4, lines 24-27 and col.6, lines 7-28; security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet. The values are compared and if valid, decryption of the packet proceeds on, but if invalid then it is discarded which inherently would not proceed further to the decryption step.)**

**As per claim 27: see col.6, lines 25-46 and FIG.6;** discusses a cryptographic engine to perform cryptographic processing on the received data.

******For further details and a better understanding of the rejections above, please refer to on Abadi, Et Al. on col.3, line 55...Et. SEQ. and its Figures.***

***Response to Arguments***

**3. *Applicant's arguments filed May 7, 2004 have been fully considered but they are not persuasive.***

The Examiner finds the arguments not persuasive pertaining to "identifying the security services", "cryptographic processing", and determining if cryptographic processing is needed to be performed.

According to the specification, the security services refers to determining the algorithm(s) to use for the service and put in place any keys to provide the requested services (pg.8, lines 5-7). Abadi teaches the security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. The packet includes the encrypted key values, the location the key is stored, and the destination address (col.4, lines 49-68 and col.9, lines 2-4). Adadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet (see col.3, lines 61-65, col.4, lines 24-46 and col.6, lines 7-28)

Further, the security information refers to information identifying encryption and/or authentication algorithms, location of keys, location or length of data to be encrypted, etc. (pg.5, lines 11-15). Abadi discloses the security information contained in the packet header such as key

location, encrypted key value, key for encryption/decryption, and destination address, all of these information identifies the security service of the data packet (col.4, lines 28-68 and col.8, line 60 thru col.9, line 4)

The cryptographic processing in the specification points out that it includes encryption and/or authentication of data before transmission to the network (pg. 4, lines 11-12 and pg.7, lines 23-25). Abadi discloses encrypting the data before transmitting to the host (col.4, lines 24-31 and col.6, lines 67-68).

Abadi also discusses determining if cryptographic processing is needed to be performed by the values being compared and if valid, decryption of the packet proceeds. But, if the values does not match to the stored values, it is considered invalid and is discarded which inherently would not proceed further to the decryption step (col.6, lines 7-28).

## ***Conclusion***

**4.** Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event

a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
RY PATE[illegible]AMINE
GY CENTE[illegible]